Подходы по совершенствованию борьбы с киберхищениями

Approaches to improving the fight against cyber theft

Фрасов А.Д.
Аспирант 2-го курса по направлению 5.1.4. Уголовно-правовые науки, ФГБОУ ВО «Ульяновский государственный университет», г. Ульяновск
e-mail: tema73rf@gmail.com

Frasov A.D.
2nd - year Postgraduate Student in the Field of 5.1.4. Criminal Law Sciences, Ulyanovsk State University, Ulyanovsk
e-mail: tema73rf@gmail.com

Аннотация
Статья посвящена исследованию специфики уголовно-правовых норм борьбы с киберхищениями. В материале приведены статистические сведения, демонстрирующие преступность в киберпространстве. Результаты научных исследований в области цифровых технологий демонстрируют рост интеграции информационно-коммуникационных и компьютерных технологий в общественные процессы, что также отражается и на доступность совершения мошеннических действий с их применением. Целью статьи является развитие теоретических подходов борьбы с киберхищениями на условиях устойчивого взаимодействия между правоохранительными органами, банковским сектором и операторами связи. Решение задач по формированию межорганизационного взаимодействия будет способствовать борьбе с интенсивной тенденцией роста киберхищений. Основная гипотеза исследования заключается в том, что цифровизация и информационно-коммуникационные технологии оказывают влияние не только на интенсивность и объемы продвижения информации, но и на экономические, социальные тенденции, в том числе и совершение преступлений. Методологическую основу исследования составляют методы логического, общенаучного, правового, статистического и сравнительного анализа. В совокупности данные методы исследования позволили обеспечить достоверность анализа и обоснованность полученных выводов. Предложена авторская концепция по устойчивому взаимодействию между правоохранительными органами, банковским сектором и операторами связи будет способствовать интеграции ресурсов и компетенций борьбы с киберхищениями.
Ключевые слова: киберпреступления, киберхищения, электронные средства платежа, удаленный доступ, информационные технологии, экспоненциальный рост, общественная опасность, уголовно-правовые, криминологические подходы, экспоненциальный рост.

Abstract
The article is devoted to the study of the specifics of the criminal law norms of combating cyberthefts. The material provides statistical data demonstrating the crime in cyberspace. The results of scientific research in the field of digital technologies demonstrate the growth of the integration of information and communication and computer technologies in social processes, which also affects the availability of committing fraudulent actions with their use. The purpose of the article is to develop theoretical approaches to combating cyberthefts on the basis of sustainable interaction between law enforcement agencies, the banking sector and telecom operators. Solving the problems of forming inter-organizational interaction will contribute to the fight against the intensive trend of cyber-thefts. The main hypothesis of the study is that digitalization and information and communication

technologies affect not only the intensity and volume of information promotion, but also economic, social trends, including the commission of crimes. The methodological basis of the study is based on the methods of logical, general scientific, legal, statistical, and comparative analysis. In combination, these research methods ensured the reliability of the analysis and the validity of the conclusions obtained. The author's concept of sustainable cooperation between law enforcement agencies, the banking sector, and telecom operators will contribute to the integration of resources and competencies in the fight against cyberthefts.
Keywords: cybercrimes, cybertheft, electronic means of payment, remote access, information technology, exponential growth, public danger, criminal law, criminological approaches, exponential growth.

Введение

Информационно-коммуникационные и компьютерные технологии стали неотъемлемой частью жизни современного общества. Современные цифровые технологии по мгновенному переводу денежных средств в режиме онлайн сильно упрощают жизнь современного общества, а также ускоряют процесс экономического взаимодействия между физическими и юридическими лицами. Однако стоит отметить, что онлайн-банкинг и социальная инженерия имеют свои уязвимые места, которые активно используются злоумышленниками для кражи денежных средств граждан.

На сегодняшний день состояние киберхищений как в мире, так и в Российской Федерации неизменно растет, при этом ситуация с киберхищениями неоднородная, остается весьма острой и требует постоянных усилий в борьбе с указанным видом преступлений.

Для разработки и реализации мероприятий по борьбе с киберпреступлениями важна их квалификация. Проблемы квалификации хищений с использованием электронных систем платежа рассматриваются в теоретическом, научном и практическом форматах, что достаточно предметно представлено в публикациях И.Р. Бегишева [2, 103], Л.В. Боровых [3, 100], О.В. Ермаковой [6, 108], М.А. Ефремовой [7, 20], Н.А. Карповой [8, 109], А.А. Лихолетова [9, 36], А.П. Перетолчина [11, 62] и других ученых.

Сопоставляя эволюцию развития информационных и телекоммуникационных технологий со статистикой оборота финансовых потоков через систему электронных средств платежа в России можно увидеть экспоненциальный рост киберпреступлений, а именно, за последние 10 лет количество киберпреступлений увеличилось 14 раз, с 55000 случаев в 2015 году до 764400 преступлений в 2024 году с резким повышением в пандемийный период, с 2019 года по 2020 год темп роста зарегистрированных случаев киберпреступлений составил 8,5 раз. Преобладание киберхищений, более 60% в общей совокупности киберпреступлений, указывает на основной мотив киберпреступлений, связанный с незаконным обогащением.

Приведенная статистика киберхищений отражает не только интенсивную динамику роста, но и преобладающую долю в общем количестве киберпреступлений. Киберхищения, совершенные в сети Интернет с помощью компьютерных технологий обладают повышенной общественной опасностью, поскольку совершаются удаленно, зачастую в формате DarkNet,- темной сети, на скрытом сегменте Интернета с применением социальных технологий и искусственного интеллекта. Таким образом, рост совершения преступных действий с использованием информационных технологий и информационно-телекоммуникационных сетей на удаленном доступе затрудняет их раскрываемость, что характеризует повышенную опасность. На фоне роста зарегистрированных случаев киберхищений показатели раскрываемости снижаются, если раскрываемость в 2010 году составляла 33%, то в 2018 году 24,8%, а с 2019 года сохраняется в пределах 22%.

Данная тенденция указывает низкую эффективность существующих уголовно-правовых и криминологических подходов борьбы с киберхищениями и необходимость мер со их совершенствованию.

Результаты

Электронные средства платежа являются одним из самых распространенных и удобных инструментов экономической деятельности как для юридических и физических лиц, а также при выполнении государстенных функций, прежде всего в области налогообложения и государственных закупок.

Инновационный процесс в банковском секторе стимулирует развитие электронных платежных систем, но поскольку в цифровую экосистему интегрированы как законопослушные клиенты, потребители банковских услуг, так и злоумышленники, то рост использования электронных средств платежа сопровождается ростом хищений денежных средств в информационной среде, в ходе совершения мошеннических действий применяется комплекс мер несанкционного вторжения в платежную систему. Исходя из этого, можно сделать вывод, что мошенничество с использованием электронных средств платежа обладает повышенной общественной опасностью, поскольку подрывает безопаснность общественных отношений и национальную безопаснсоть, что предопределяет актуальность концепции уголовной ответственности за хищения с использованием электронных средств платежа.

Следует заметить, что развитию финансовых операций, осуществляемых посредством электронных средств характерна уязвимость от опасного воздействия преступных посягательств мошенников с применением вредоносных программ, что указывает на серьезную проблему развития общественных отношений и в целом национальную безопасность на фоне роста киберпреступлений. Для реализации преступных действий злоумышленники применяют вредоносное программное обеспечение, фишинговые сайты, электронные платформы, используют подменные номера, также проверенное временем доверие наших граждан позволяет преступниками создавать финансовые пирамиды.

Уровень киберхищений доминирует в общем объеме краж и составляет более 70%, что демонстрирует транзакционность развития общественных отношений в существующих реалиях.

Статистика мошенничества с использованием электронных средств платежа характеризуется интенсивной динамикой, высоким удельным весом в структуре киберпреступлений и большим ущербом, причиняемого субъектам финансовых операций. Хищения, совершаемые дистанционно, наносят существенный урон экономике, имущественной безопасности граждан и организаций. Ущерб от таких преступлений только за 2021 г. превысил 67 млрд руб. Значительную часть ущерба от хищений, совершаемых дистанционно, объективно формируют посягательства, совершаемые с применением высокотехнологичных программных и технических средств. Вместе с тем не меньшую опасность несут в себе менее технологичные, но значительно более распространенные дистанционные хищения, совершаемые с использованием средств мобильной связи [10, 152].

Стоит отметить, что в последнее время помимо «классического» интернет-мошенничества, активно стали развиваться кибер-атаки на базы данных организаций, что приводит к значительным убыткам данных юридических лиц. Так в 2024 году убытки организаций, зарегистрированных в РФ, от кибер-атак на базы данных указанных юридических лиц составили порядка 4,88 млн. долларов США.

Динамика роста киберпреступлений отражает экспоненциальность роста, а именно темп роста за последние 10 лет составил 14 раз, с 5572 случаев в 2008 году до 764400 преступлений в 2024 году. Резкий взлет произошел в период 2019-2020 года, в пандемийный период. Динамика зарегистрированных киберпреступлений за период 2008 по 2024 года представлена на рисунке [12].

В 2024 году рост количества «киберхищений» на территории Российской Федерации составил около 15% в сравнении с предыдущим годом, общий ущерб от указанного вида преступлений составил примерно 168 млрд. рублей, а средняя сумма каждого «киберхищения» около 219493 рублей.

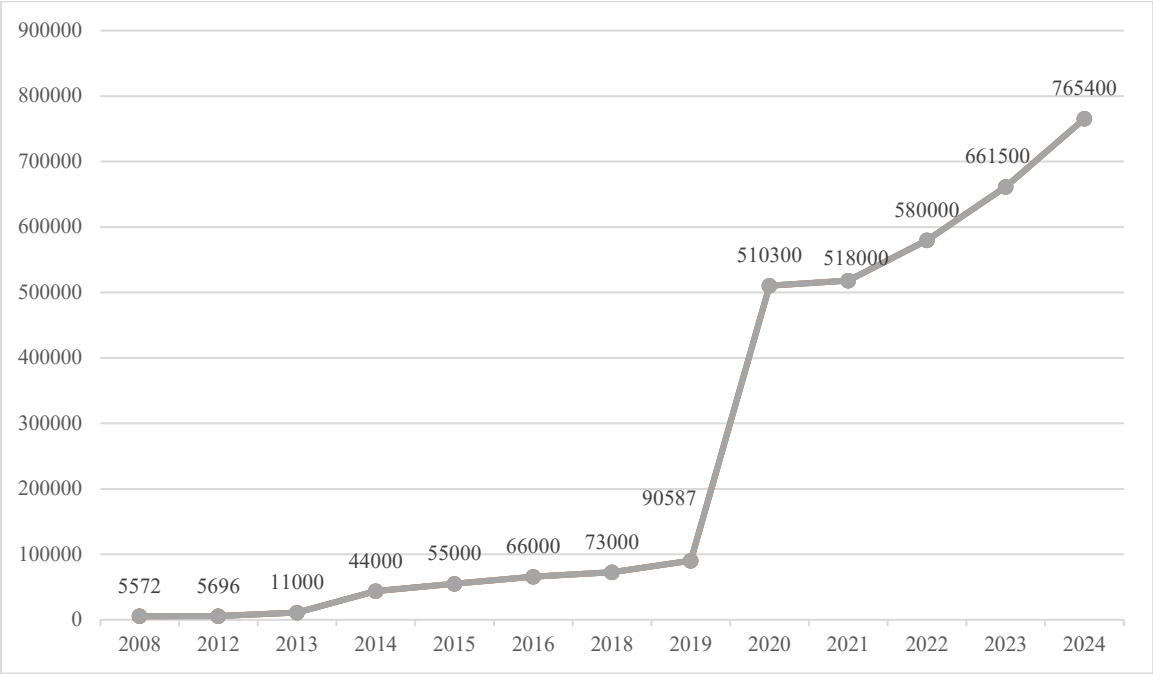

Рис.1. Динамика зарегистрированных киберпреступлений за период 2008г. по 2024гг.

Ущерб от совершения киберхищений по своему размеру далеко не всегда сопоставим с более технологичными хищениями, но вред от них не менее, а иногда и более серьезный, так как причиняется зачастую незащищенным категориям граждан [10, 152]. Рост киберпреступлений на фоне инфляции и понижения платежеспособности жертв от подобных преступлений указывает на высокую общественную опасность преступлений, совершаемых в глобальной сети Интернет посредством информационно-коммуникационных технологий.

В условиях современных реалий одним из опасных преступлений являются киберхищения, которые охватывают широкий диапазон действий, связанных с применением информационных технологий, в том числе и мошенничество с использованием электронных средств платежа.

Рис.2. Способы совершения киберхищений

На рисунке 2 представлена классификация мошенничество с использованием электронных средств платежа (рис.2).

Рассматривая структуру «киберпреступлений», необходимо затронуть тот факт, что дистанционные хищения и мошенничества значительно преобладают в данной совокупности. За 2024 год из 765400 зарегистрированных киберпреступлений 486000 случаев, то есть, 64% - составили киберпреступления, относящиеся к дистанционным хищениям и интернет-мошенничеству. Данные обстоятельства детерминирующих или иным образом способствующих процессу превращения личности в жертву преступления [4, 157].

Структура киберхищений за 2024 год представлены на рисунке 3 [11]. По данным структуры очевидно, что доля мошенничества с использованием электронных средств платежа преобладает в общем количестве киберхищений.

Рис.3. Структура киберпреступлений в 2024 году

В общей совокупности киберпреступления осуществляются в широком диапазоне, из которых доля киберхищений составляет более 60%:

- основная доля приходится на мошенничество 37% (ст. 159, 159.3, 159.6 УК РФ);
- кражи, 30% (ст.158 УК РФ);
- немного меньше - преступления, связанные с незаконной организацией и проведением азартных игр, доля которых в общей совокупности составляет 33% (ст.172.1 УК РФ);
- деяния по незаконному производству, сбыту (пересылкой наркотических средств, психотропных веществ), а также незаконным сбытом или пересылкой растений, содержащих наркотические средства или психотропные вещества (ст. 228.1 УК РФ) [12];
- 1% - преступления по изготовлению порнографических материалов (ст. 242, 242.1, 242.2 УК РФ), призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганды терроризма (ст. 205.2 УК РФ) [12];
- призывы к осуществлению экстремистской деятельности (ст. 280 УК РФ).

В силу совершения киберпреступлений на удаленном доступе, зачастую в формате DarkNet (темная сеть, скрытый сегмент Интернета) уровень раскрываемости киберпреступлений остается одним из низких, не превышая 25%.

Полиция начинает работать с заявителем, когда преступление совершено, как говорится, «по факту» [13], к тому же, материально-техническое обеспечение, уголовно-правовые меры, шаблонность оперативных и следственных мероприятий в данной области сдерживает показатели раскрываемости и профилактику мошенничества с использованием электронных средств платежа.

В Российской Федерации правовое регулирование информационного пространства осуществляется посредством Конституции Российской Федерации и федеральных законов.

Активное освоение и внедрение информационных технологий в общественные отношения и рост совершенных преступлений в информационном поле послужило основанием для разработки Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». В данном документе представлены подходы и принципы государственной политики в области информационной безопасности, в том числе защиты персональных данных и государственной тайны.

С 2014 года актуальным аспектом в области информационной безопасности является «цифровой суверенитет», то есть право государства на независимое управление цифровыми ресурсами, развитие цифровой инфраструктуры в соответствии с национальными интересами, что предопределило разработку Стратегии кибербезопасности РФ, а с 2021 года в соответствии с Указом Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» она реализуется.

Диапазон правовых норм приведен на рисунке 4.

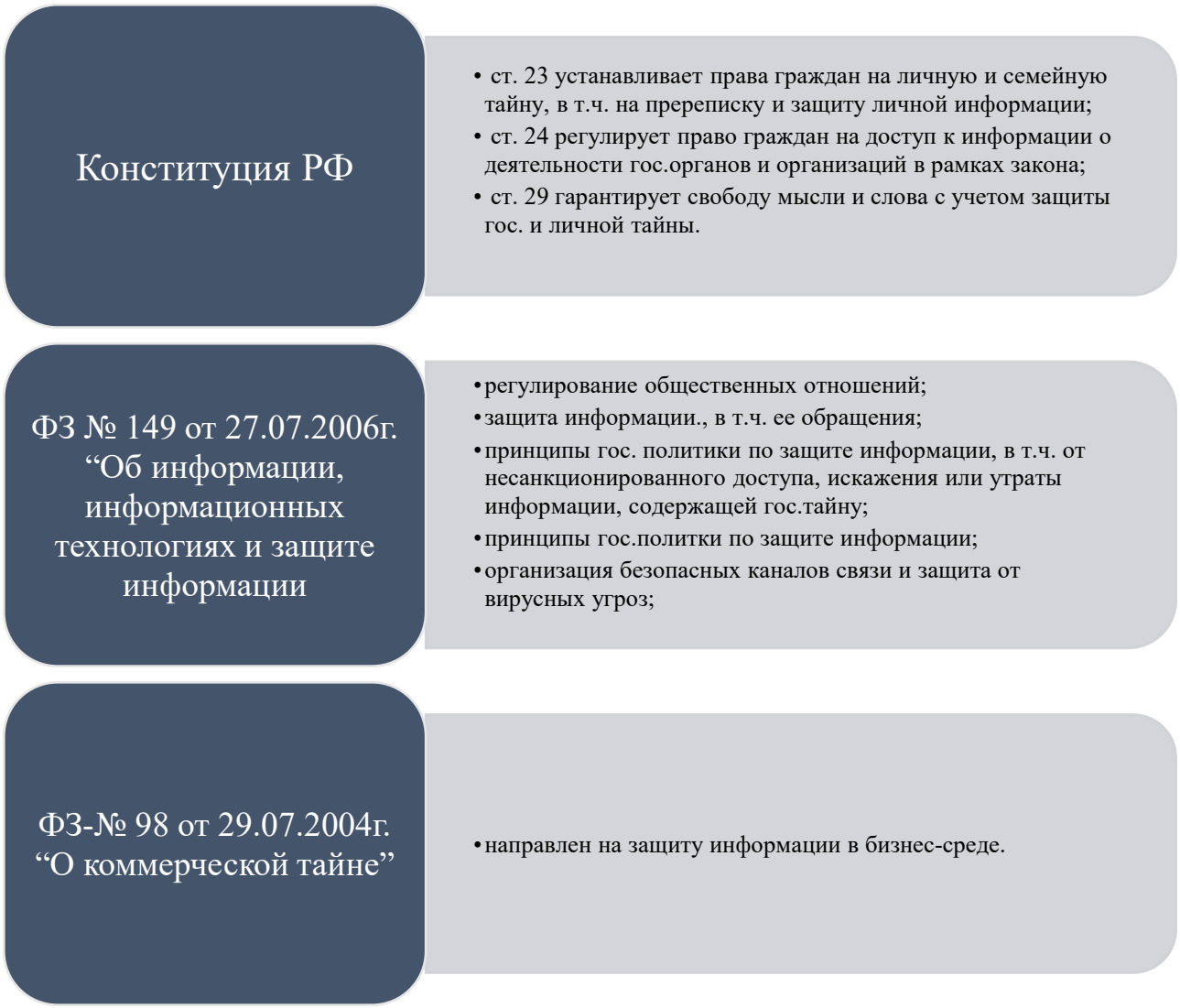

Рис.4. Правое регулирование информационного пространства

В Федеральном законе №41–ФЗ от 01.04.2025 года «О защите граждан от кибермошенничества» достаточно конкретно обозначены подходы по обмену информацией между операторами связи и правоохранительными органонами. В данном аспекте следует отметить, что с 2021 года информационно-коммуникационные технологии существенно актуализировались, и злоумышленники преуспевают в информационно-психологическом давлении, дистабилизируя информационную безопасность, тем самым нанося ущерб обществу и государству.

Исходя из тенденций современных преобразований очевидно, что правовой механизм в области информационной безопасности в настоящее время находится в стадии формирования и инструменты по предупреждению киберпреступлений осваиваются последовательно относительно данных преступных проявлений. Указанные обстоятельства подчеркивают актуальность научного осмысления проблем квалификации и пресечения деятельности преступных групп, специализирующихся на киберпреступлениях, в том числе и совершении мошеннических действий с использованием электронных средств платежа [14].

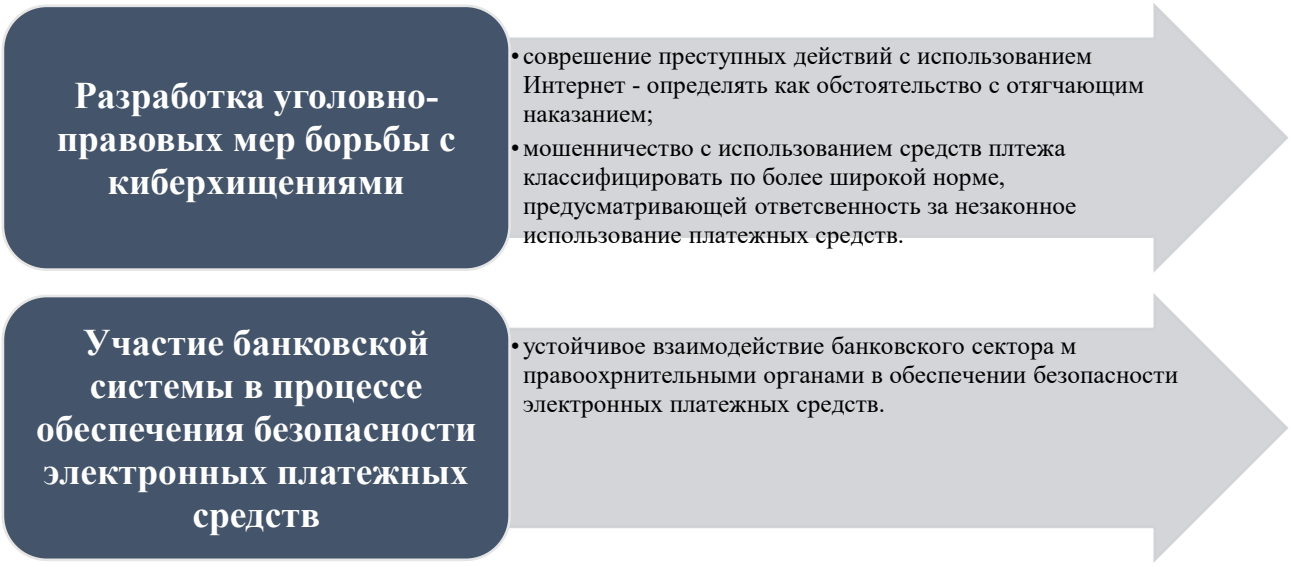

Рис.5. Подходы по борьбе с мошенничеством с использованием электронных средств платежа

Для реализации конкретных мер по борьбе с кибермошенничеством следует подойти комплексно, то есть важна актуализация как уголовно-правовых мер, так и задействование банковской системы в процессе обеспечения безопасности транзакций (рис.5).

Для разработки актуальных уголовно-правовых мер борьбы с мошенничеством с использованием электронных средств платежа важно знать причины и условия данных проявлений, а также интересы субъектов информационного пространства, а именно: государства, юридических и физических лиц. Данные аспекты будут способствовать целенаправленным действиям по разработке и актуализации норм права по защите интересов субъектов правового поля.

В соответствии с дополнениями и изменениями Уголовного кодекса Российской Федерации следует, что совершение преступных действий с использованием информационно-телекоммуникационных сетей, в том числе и сети «Интернет» определяется как обстоятельство, отягчающее наказание. В соответствии с чем полагаем, что ужесточение ответственности за допущение утечек данных и отнесение мошенничества с использованием информационных технологий к отягчающим обстоятельствам, будет способствовать назначению справедливого наказания.

Очевидно, что для обеспечения функционирования платежной системы необходим координатор, имеющий компетенции и полномочия по организации электронных платежей и разрешения споров по транзакциям. Данным субъектом является банк, осуществляющий деятельность в соответствии с лицензией, предоставленной Центральным банком России. Полагаем, что одним из подходов по устранению причин и условий, способствующих росту с кибермошенничества в большей степени находится в компетенции регуляторов, операторов связи, банков и интернет-провайдеров. Для стабилизации ситуации необходимо устойчивое взаимодействие между правоохранительными органами, банковским сектором и операторами связи. Благодаря электронному документообороту такое взаимодействие вполне возможно и

будет способствовать оперативному реагированию на незаконные действия, принятию своевременных предупредительных мер по их блокировке, что в целом обеспечит информационную безопасность всех участников системы.

Обсуждение и выводы

В соответствии с представленным описанием очевидно, что тенденция развития киберпреступлений является опасным и во многом еще неизвестным явлением для современного общества, а квалификация киберхищений, разработка современного правового механизма, а также устойчивое взаимодействие между правоохранительными органами, банковским сектором и операторами связи - приоритетной задачей в борьбе с киберпреступностью. Применение комплекса мер, как организационных, так и правовых, будут способствовать стабилизации ситуации.

Литература

1. Уголовный кодекс Российской Федерации: Федеральный закон от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации. – 1996. – № 25. – Ст. 2954.
2. Бегишев И.Р. Преступления в сфере обращения цифровой информации / И.Р. Бегишев, И.И. Бикеев. – Казань: Познание, 2020. – 300 с.
3. Боровых Л.В. Направленность обмана в составе мошенничества с использованием платежных карт / Л.В. Боровых, Е.А. Корепанова // Вестник Пермского университета. Юридические науки. – 2016. – № 1 (31). – С. 98–104.
4. Вишневецкий К.В. Виктимизация: факторы, условия, уровни / К.В. Вишневецкий // Теория и практика общественного развития. – 2014. – № 4. – С. 226–227.
5. Гринько С.Д. уголовно-правовое противодействие финансированию терроризма // право и государство: теория и практика. 2019. № 4(172) с.88-91.
6. Ермакова О.В. Вопросы квалификации мошенничества с использованием электронных средств платежа (ст. 1593 УК РФ) в свете изменений уголовного закона / О.В. Ермакова // Вестник Барнаульского юридического института МВД России. – 2018. – № 2 (35). – С. 108–109.
7. Ефремова М.А. Мошенничество с использованием электронной информации/ М.А. Ефремова // Информационное право. – 2013.–№ 4.–С.19–21.
8. Карпова Н.А. Уголовно-правовая характеристика и проблемы квалификации мошенничества с использованием платежных карт / НА. Карпова, Я.С. Калининская // Проблемы экономики и юридической практики. – 2017. – № 5. – С. 145–148.
9. Лихолетов А.А. Проблемы разграничения мошенничества с использованием платежных карт с другими составами преступлений / А.А. Лихолетов // Российская юстиция. – 2017. – № 6. – С. 35–37.
10. Мироненко С.Ю. Понятие и методы виктимологического предупреждения преступности Виктимология 2021, Т. 8, № 2. С. 149–155.
11. Перетолчин А.П. Способ совершения мошенничества с использованием электронных средств платежа / А.П. Перетолчин // ГлаголЪ правосудия. – 2019. - №4(22). – С.60-63.
12. Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2024 года // Официальный сайт Министерства внутренних дел Российской Федерации. URL: https://мвд.рф/reports/item/22678184/ (дата обращения: 26.07.2025).
13. Число_киберпреступлений_в_Россииhttps://www.tadviser.ru/index.php/
14. Онлайн проект «Обзор электронной коммерции». [Электронный ресурс] // URL:https://elcomrevue.ru/blog/cybercrime/kibeoprestupnost-chto-eto (дата обращения: 18.08.2025).